UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------x

IN RE UNIVERSITY UROLOGY DATA SECURITY INCIDENT LITIGATION

No. 23-CV-06484-LTS

----------x

MEMORANDUM ORDER

Plaintiffs Joseph DiAmbrose and Andres Viva ("Plaintiffs") bring an eight-count putative class action Consolidated Complaint against Defendant Jed C. Kaminetsky, M.D., P.C. d/b/a "University Urology" and "University Urology Associates" ("Defendant" or "Universal Urology"), alleging that Defendant failed to secure and safeguard Plaintiffs' personally identifiable information and protected health information from unauthorized third-party hacking and exfiltration. (Docket entry no. 28 ("Consol. Compl.").) Plaintiffs bring claims for negligence, breach of contract, breach of implied contract, unjust enrichment, breach of confidence, breach of New York's Information Security Breach and Notification Act, deceptive acts and practices in violation of New York General Business Law section 349, and false advertising in violation of New York General Business Law section 350.

Before the Court is Defendant's motion to dismiss the Consolidated Complaint under Federal Rule of Civil Procedure 12(b)(1) for lack of subject matter jurisdiction and Rule 12(b)(6) for failure to state a claim upon which relief can be granted. (Docket entry no. 29.) The Court has carefully considered the parties' submissions—(docket entry no. 29-1 ("Def. Mem."); docket entry no. 30 ("Pl. Opp."); docket entry no. 31 ("Def. Reply")[1])—and, for the following reasons, Defendant's motion is denied.

[1] Docket entry pincites are to ECF-designated pages.

BACKGROUND

For purposes of this motion practice, the Court accepts all well-pleaded allegations in the Complaint as true and draws all reasonable inferences in Plaintiffs' favor.

On or around February 1, 2023, Defendant suffered a data breach. (Consol. Compl. ¶ 2.) Defendant's internal data systems were breached by unauthorized third-party hackers, who "accessed and exfiltrated" Plaintiffs' and putative class members' personal information. (Id. ¶ 2.) Plaintiffs allege that 56,816 individuals were affected by the data breach. (Id.) On May 1, 2023, Plaintiffs received data breach notices informing them of the incident, advising them of steps that should be taken to protect their identity, and offering two years of credit monitoring services. (Id. ¶¶ 17-18.)

Plaintiffs allege that they face an "imminent, immediate, and continuing risk of harm from identity theft and identity fraud," especially given the sensitive nature of the stolen data. (Id. ¶ 59.) According to Plaintiffs, to mitigate these risks, they must continuously monitor their accounts, purchase credit and identity theft monitoring services, and expend additional time and effort to prevent and mitigate potential future losses. (Id.) Plaintiffs claim that they have already spent time dealing with the increased risk of fraud and monitoring their accounts for fraud and that they anticipate spending considerable time and money "on an ongoing basis" in the future. (Id. ¶ 60.) Plaintiffs also claim they have "lost the value of their PII [personally identifiable information] and PHI [protected health information]." (Id. ¶¶ 6, 62.)

Furthermore, Plaintiff Vivas alleges that he experienced actual injury in the form of identity theft resulting from the data breach. (Id. ¶ 61.) Vivas alleges that, in October 2023, an unauthorized user opened a credit card in his name using the personal information compromised in the data breach. (Id.) "[N]ot long after" the data breach, he was also notified of

two fraudulent transactions totaling $1,600. (Id.) Finally, he alleges an increase in suspicious spam phone calls and text messages since the breach. (Id.)

DISCUSSION

Defendant moves under Federal Rule of Civil Procedure 12(b)(1) and 12(b)(6). With respect to the former provision, Defendant contends that Plaintiffs lack standing because the Plaintiffs fail to allege a cognizable injury-in-fact. With respect to the latter, Defendant argues that Plaintiffs fail to allege that any extraction occurred and that there is no logical nexus between the data breach and the alleged identity theft experienced by Plaintiff Vivas.

None of Defendant's arguments are availing for the reasons explained below. First, Plaintiffs have sufficiently pleaded injury-in-fact based on the substantial risk of future identity theft or fraud. Second, Plaintiffs allege sufficiently that their personal information was "exfiltrated" and "stolen" and that the alleged identity theft was causally connected to the data breach. Defendant's motion to dismiss is, therefore, denied in its entirety.

Article III Standing

"Where, as here, the defendant moves for dismissal under Rule 12(b)(1), Fed. R. Civ. P., as well as on other grounds, 'the court should consider the Rule 12(b)(1) challenge first.'" Rhulen Agency, Inc. v. Ala. Ins. Guar. Ass'n, 896 F.2d 674, 678 (2d Cir. 1990) (citation omitted). "In resolving a motion to dismiss under Rule 12(b)(1), the district court must take all uncontroverted facts in the complaint (or petition) as true, and draw all reasonable inferences in favor of the party asserting jurisdiction." Tandon v. Captain's Cove Marina of Bridgeport, Inc., 752 F.3d 239, 243 (2d Cir. 2014).

Defendant argues that the Court lacks subject matter jurisdiction because Plaintiffs lack standing. To establish standing, Plaintiffs must demonstrate (1) that they suffered

an injury in fact that is concrete, particularized, and actual or imminent, (2) that the defendant caused the injury, and (3) that the requested judicial relief would likely redress the injury. McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 299-300 (2d Cir. 2021). "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss[,] we presume that general allegations embrace those specific facts . . . necessary to support the claim." Lujan v. Defs. of Wildlife, 504 U.S. 555, 561 (1992) (internal quotations and citation omitted). The Court considers each of the three requirements in turn and finds them all satisfied.

Injury-In-Fact

Plaintiffs must allege a "concrete, particularized, and actual or imminent [injury]." Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013). "[A]llegations of possible future injury" or even an "objectively reasonable likelihood" of future injury are insufficient to confer standing. Id. at 409-10. Instead, a future injury constitutes an injury-in-fact only "if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014).

Plaintiffs allege that they, and the putative class members, face an "imminent, immediate, and continuing risk of harm from identity theft and identity fraud," especially given the sensitive nature of the stolen data. (Consol. Compl. ¶ 59.) According to Plaintiffs, to mitigate these risks, they will need to continuously monitor their accounts, purchase credit and identity theft monitoring services, and expend additional time and effort to prevent and mitigate potential future losses. (Id.)

Where, as here, plaintiffs allege that they "are at an increased risk of identity theft or fraud based on an unauthorized data disclosure," the Second Circuit has instructed courts to

consider several factors, including: "(1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." McMorris, 995 F.3d at 303. Here, all three McMorris factors weigh in favor of finding standing.

First, Plaintiffs allege "that healthcare providers such as Defendant are specifically targeted by hackers due to the value of the PII/PHI [personally identifiable information/protected health information] that they collect and maintain as a part of their ordinary course of business." (Consol. Compl. ¶ 31.) As the Seventh Circuit explained in the context of a cyberattack of a department store's customer database, "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015). That same reasonable inference applies here: it is reasonable to infer that hackers targeted a medical practice specifically to obtain the personal information of patients.

Second, Plaintiff Vivas alleges that, as a result of the data breach, he has been the victim of identity theft. (Consol. Compl. ¶ 61.); see In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 58 (D.C. Cir. 2019) ("[T]he fact that certain Arnold Plaintiffs have already had fraudulent accounts opened and tax returns filed in their names moves the risk of future identity theft across the line from speculative to substantial, at least at this early stage in the proceedings."). Vivas alleges that, eight months after the data breach, an unauthorized user opened a credit card in his name using the information compromised in the data breach, and that

"not long after" the breach, he was notified of two fraudulent transactions totaling $1,600. (Consol. Compl. ¶ 61.) He also alleges an increase in suspicious spam phone calls and text messages since the breach. (Id.); see In re Canon U.S.A. Data Breach Litig., No. 20-CV-06239-AMD-SJB, 2022 WL 22248656, at *5 (E.D.N.Y. Mar. 15, 2022) (finding in favor of plaintiffs on second factor where "plaintiffs allege that since the Data Breach, they have 'experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages'" (citation omitted)).

Admittedly, Plaintiff DiAmbrose does not allege any identity theft resulting from the data breach. Similarly, Plaintiffs do not allege that every putative class member has experienced identity theft caused by the data breach or limit the putative class to those who have experienced actual identity theft. See TransUnion LLC v. Ramirez, 594 U.S. 413, 431 (2021) ("Every class member must have Article III standing in order to recover individual damages."). This, however, does not divest them of standing. An allegation of "known misuse of information in the dataset accessed in the hack" "is not necessary to establish that an injury is sufficiently imminent to constitute an injury in fact." Bohnak v. Marsh & McLennan Cos., Inc., 79 F.4th 276, 289 (2d Cir. 2023). This is especially true "where some part of the compromised dataset has been misused—even if a plaintiff's own data has not." Id. at 288. For example, "although the specific plaintiffs in [a] case had not experienced any fraudulent activity, allegations that *other* customers whose data was compromised in the same data breach had reported fraudulent charges on their credit cards helped establish that the plaintiffs were at a substantial risk of future fraud." McMorris, 995 F.3d at 301-02 (2d Cir. 2021) (emphasis in original) (citing In re Zappos.com, Inc., 888 F.3d 1020, 1027 & n.7 (9th Cir. 2018)). Consequently, the allegation that Plaintiff Vivas has experienced identity theft advances Plaintiff DiAmbrose's risk of future

identity theft across the line from speculative to substantial, as well as that of other putative class members.

Third, the information exposed in the data breach is sensitive, high-risk data susceptible to identity theft or fraud. (Consol. Compl. ¶ 2) (describing the breached information as "names, addresses, dates of birth, username/email in combination with a password or security question that would allow access to an online account, medical condition information, medical treatment information, medical treatment results, prescription information, health insurance policy numbers, subscriber identification numbers, health plan beneficiary numbers and billing/invoice information")); see McMorris, 995 F.3d at 302 ("Naturally, the dissemination of high-risk information such as Social Security numbers and dates of birth—especially when accompanied by victims' names—makes it more likely that those victims will be subject to future identity theft or fraud." (citation omitted)).

All three McMorris factors favor Plaintiffs. Defendant's only argument in opposition is that Plaintiffs fail to allege that hackers ever "extracted" any personal data from Defendant's computers. (Def. Mem. at 6.) Thus, Defendant avers, the risk of future identity theft is too speculative to support standing. (Id.) This argument fails because Plaintiffs do allege extraction: Plaintiffs allege that their data was "exfiltrated" and "stolen" by unauthorized third parties. (Consol. Compl. ¶¶ 7, 16; see infra pp. 10-11 (discussing this argument in more detail).)

Accordingly, Plaintiffs have established injury-in-fact based on the substantial risk of future identity theft or fraud.[2]

Traceability and Redressability

While Defendants advance no argument on traceability or redressability, the Court considers these prongs sua sponte and finds them satisfied. See Sharkey v. Quarantillo, 541 F.3d 75, 88 (2d Cir. 2008) (Courts are "required to raise" threshold jurisdictional issues "sua sponte." (citing Arbaugh v. Y & H Corp., 546 U.S. 500, 514 (2006))).

Traceability requires the plaintiff to "demonstrate a causal nexus between the defendant's conduct and the injury." Chevron Corp. v. Donziger, 833 F.3d 74, 121 (2d Cir. 2016). "Traceability is a lower bar than proving causation on the merits."[3] In re Unite Here Data Sec. Incident Litig., 740 F. Supp. 3d 364, 376 (S.D.N.Y. 2024) (citing Vt. Agency of Nat. Res. v. United States ex rel. Stevens, 529 U.S. 765, 771 (2000)). So long as there is a "'fairly . . . trace[able]' connection between the alleged injury in fact and the alleged conduct of the defendant[,]" traceability can be satisfied. Vt. Agency, 529 U.S. at 771 (quoting Simon v. Eastern Ky. Welfare Rts. Org., 426 U.S. 26, 41 (1976)).

---

[2] Plaintiffs also allege "actual injury in the form of time spent dealing with the Data Breach and increased risk of fraud resulting from the Data Breach and/or monitoring their accounts for fraud." (Consol. Compl. ¶ 60.) Because Plaintiffs have adequately alleged a "substantial risk of future identity theft or fraud," this injury is also cognizable as an injury-in-fact. McMorris, 995 F.3d at 303 ("[W]here plaintiffs have shown a substantial risk of future identity theft or fraud, 'any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact.'" (quoting In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 59 (D.C. Cir. 2019))).

[3] Relatedly, although separately, Defendant argues, in support of its Rule 12(b)(6) motion, that Plaintiffs failed to plead causation, which is a required element for some of Plaintiffs' claims. This argument fails for the reasons discussed below. (Infra pp. 11-12.)

Plaintiffs have established traceability. Plaintiff Vivas alleges that, in October 2023, approximately eight months after the data breach, "an unauthorized user opened a credit card in his name using the Private Information compromised in the Data Breach." (Consol. Compl. ¶ 61.) With respect to Plaintiff DiAmbrose and other putative class members who did not allege subsequent identity theft, their alleged harm is the increased risk of future identity theft, which is traceable to the data breach. See In re GE/CBPS Data Breach Litig., No. 20-CV-02903-KPF, 2021 WL 3406374, at *4 n.2 (S.D.N.Y. Aug. 4, 2021) ("Plaintiff adequately alleges that the injuries he suffered [of the increased risk of future identity theft or fraud] are 'fairly traceable' to Defendants' actions in collecting and storing PII without following proper data security principles or implementing adequate cyber security measures.").

Finally, Plaintiffs must show that a favorable resolution of their case would redress their alleged injuries. Lujan, 504 U.S. at 560. That criterion is satisfied because damages could compensate Plaintiffs' injuries, and because injunctive relief, such as requiring the provision of credit monitoring, could limit the extent of any risk of future injuries. See In re GE/CBPS, 2021 WL 3406374, at *4 n.2.

Accordingly, Plaintiffs have established standing. Defendant's motion to dismiss the Consolidated Complaint for lack of subject matter jurisdiction is denied.

Whether Plaintiffs Have Stated a Claim

To survive a Rule 12(b)(6) motion to dismiss, a complaint must plead "enough facts to state a claim to relief that is plausible on its face." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). A proper complaint cannot simply recite legal conclusions or bare elements of a cause of action; factual content must be pleaded that "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 556 U.S.

662, 678 (2009). The Court accepts as true the nonconclusory factual allegations in the Complaint and draws all reasonable inferences in the Plaintiffs' favor. Roth v. Jennings, 489 F.3d 499, 501 (2d Cir. 2007).

Defendant raises two arguments in support of its motion to dismiss. The Court takes each in turn, finding neither meritorious.

Whether Plaintiffs Pleaded "Extraction" of Their Information

First, Defendant argues that Plaintiffs fail to allege that any personal data was "extracted" in the data breach. (Def. Mem. at 9-10.) This argument is meritless. Plaintiffs allege that their personal information was "exfiltrated" by hackers, and that "patient information was stolen." (Id. ¶¶ 2,7 (emphasis added).) "Exfiltrate" means "to steal (sensitive data) from a computer (as with a flash drive)." Exfiltrate, MERRIAM-WEBSTER DICTIONARY, https://perma.cc/2C2C-Q8ES (last visited Mar. 31, 2025); see also Exfiltrate, THE FREE DICTIONARY, https://perma.cc/9JSY-HGFQ (last visited Mar. 31, 2025) ("to remove (data) from a computer, network, etc surreptitiously and without permission or unlawfully"). Clearly, Plaintiffs have alleged that hackers extracted their data and that their data was stolen. Plaintiffs need not use the magic word "extracted."

Moreover, at this preliminary stage, Plaintiffs do not need to proffer evidence of how precisely the hackers breached Defendant's data systems or how exactly the hackers stole data. See Twombly, 550 U.S. at 555 ("[A] complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations."). Indeed, it is unlikely that Plaintiffs even have access to such evidence that is exclusively in Defendant's possession. Zuma Press, Inc. v. Getty Images (US), Inc., No. 16-CV-06110-AKH, 2017 WL 2829517, at *3 (S.D.N.Y. June 29, 2017) ("Where relevant information is exclusively in the possession of the defendant, as is the

case here, a plaintiff may allege facts on information and belief, and need not plead more specific facts that are unavailable to the plaintiff as a result of the defendant's own conduct.").

Even had Plaintiffs not explicitly alleged that their personal information had been "exfiltrated" and "stolen," it would be reasonable to infer that hackers who accessed data would also extract such data. Why else would hackers target and hack a medical practice, but to extract personal information? See Remijas, 794 F.3d at 693 ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

Whether Plaintiffs Pleaded Causation

Next, Defendant argues that Plaintiffs fail to allege a "nexus between the data incident and the supposed damages that [the Consolidated Complaint's] factual allegations proffer." (Def. Mem. at 10-12.) Unlike traceability, this argument goes to the merits of Plaintiffs' claims, many of which require a showing of causation. See Resnick v. AvMed, Inc., 693 F.3d 1317, 1325 (11th Cir. 2012) (Claims such as negligence, breach of contract, and breach of implied contract "require[] a plaintiff to show that the defendant's challenged action *caused* the plaintiff's harm[.]" (applying Florida law) (emphasis in original)).

To establish a causal relationship between a data breach and actual identity theft or fraud, "the pleadings must include allegations of a nexus between the two instances beyond allegations of time and sequence." Id. at 1326. A plaintiff meets this burden when he alleges that the sensitive information stolen in a data breach is the same information used to facilitate the fraud that he subsequently suffered. Id. at 1327. Plaintiff Vivas alleges exactly this—he alleges that, eight months after the data breach, "an unauthorized user opened a credit card in his name using the Private Information [that was] compromised." (Consol. Compl. ¶ 61.)

With respect to Plaintiff DiAmbrose and other putative class members, who did not allege subsequent actual identity theft, their alleged injury is the increased risk of future identity theft, which they adequately allege was caused by the data breach. See (Consol. Compl. ¶¶ 50-52, 57-66); Flores-Mendez v. Zoosk, Inc., No. 20-CV-04929 WHA, 2021 WL 308543, at *4 (N.D. Cal. Jan. 30, 2021) (finding causation allegations sufficient to survive a motion to dismiss when the complaint alleged a data breach occurred and additional information about security system was likely held by the defendant).

CONCLUSION

For the foregoing reasons, the Defendant's motion to dismiss the Consolidated Complaint under Rules 12(b)(1) and 12(b)(6) is denied. This Memorandum Order resolves Docket Entry No. 29. The above-entitled action will be referred to a Magistrate Judge for general pretrial management (including scheduling, discovery, non-dispositive pretrial motions, and settlement). An order to that effect will follow entry of this Memorandum Order.

SO ORDERED.

Dated: New York, New York
March 31, 2025

/s/ Laura Taylor Swain
LAURA TAYLOR SWAIN
Chief United States District Judge